REMARKS

In response to the Final Office Action of April 14, 2010, and in response to the

Request for Continued Examination file herewith, claims 64, 72, 77-80, 87, 88, 93, 94 and

109 have been amended. Claims 64-94 and 109 are pending in the application.

In paragraph 4 on page 2 of the Office Action, claims 64-109 were rejected under

35 U.S.C. §112, first paragraph, as failing to comply with the written description

requirement.

Applicant respectfully traverses the rejection.

Applicant respectfully submits that the claim language is fully supported by the

specification. Fig. 1 illustrates the ISP "point-of-presence" (POP) that includes an ISP POP

Server 16 (page 6, lines 2-3). Fig. 3 illustrates the data collection component of the system,

which resides at the POP server 16. The data collection component includes a sniffer 31

that monitors user-to-Internet traffic. When the sniffer 31 detects an outgoing Web page

request from a client 10, it captures the associated packets, extracts the actual URL request,

and stores it in the database 30 along with the client's IP address (page 7, lines 8-20). The

summary of the invention describes a system for accurately and anonymously profiling

Web users (page 3, lines 2-3). To correlate an IP address with the associated client, the

data collection component queries an IP address to anonymous user ID (AID) cross-

reference table stored in another database at the ISP POP (page 7, lines 8-20).

Thus, the specification describes a sniffer 31 for monitoring packets at an Internet

Service Provider (ISP) point of presence (POP). The specification also describes that the

sniffer 31 detects Web page requests and thus describes identifying monitored packets

associated with Web page requests. The specification further describes the POP server 16

anonymously profile Web users. The sniffer 31 captures packets without the user's

knowledge. Thus, the sniffer anonymously captures, at the Internet Service Provider (ISP)

point of presence (POP), packets identified as being associated with Web page requests.

Accordingly, Applicant respectfully submits that the claims and specification

comply with the written description requirement.

In paragraph 6 on page 3 of the Office Action, claims 95-108 were rejected under

35 U.S.C. §101 because the claimed invention was directed to non-statutory subject matter.

Applicant respectfully traverse the objection to the claims, but in the interest of

expediting prosecution has canceled claims 95-108 thereby rendering the rejection moot.

In paragraph 8 on page 3 of the Office Action, claims 64-71, 77, 80-87, 93, 95-101,

107 and 109 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Roth in

view of Armbruster and in further view of Bull.

In paragraph 9 on page 8 of the Office Action, claims 72-75, 79, 88-91 and 102-105

were rejected under 35 U.S.C. § 103(a) as being unpatentable over Roth in view of

Armbruster and Bull, and in further view of Sheena.

In paragraph 10 on page 11 of the Office Action, claims 76, 92 and 106 were

rejected under 35 U.S.C. § 103(a) as being unpatentable over Roth in view of Armbruster

and Bull, and in further view of Eldering.

In paragraph 11 on page 12 of the Office Action, claims 78, 94 and 108 were

rejected under 35 U.S.C. § 103(a) as being unpatentable over Roth in view of Armbruster

and Bull, and in further view of Park.

Applicant respectfully traverses the rejection.

Independent claim 64 sets forth a method that includes monitoring packets at an

Internet Service Provider (ISP) point of presence (POP), identifying monitored packets

associated with Web page requests, anonymously capturing, at the Internet Service

Provider (ISP) point of presence (POP), packets identified as being associated with Web

page requests, extracting, at the ISP POP, a Uniform Resource Locator (URL) of the

requested Web page and an IP address of the packets identified as being associated with

the Web page request, processing the extracted IP address to correlate the extracted IP

address with a user identifier using a cross-reference table at the ISP POP, associating

each extracted URL with the user identifier correlated with the extracted IP address, for

each user identifier correlated with the extracted IP address, storing the URL of the

requested Web page and the user identifier correlated with the extracted IP address at the

ISP POP, developing a user profile for the user identifier, at the ISP POP, based on the

extracted URLs associated with Web pages stored at the ISP POP and requested by the

user identifier and cross referencing Web site profiles with the extracted URLs associated

with Web pages requested by the user identifier to generate an updated user profile, at the

ISP POP, based on inferred user demographics of the Web sites requested by the user

identifier. Independent claims 80 and 109 set forth similar elements.

Roth discloses a system that provides advertisements from an advertisement server

in response to a user accessing a web site having an HTML reference to the advertisement

server. Information contained in cookies is used to update the client history.

However, Roth fails to disclose, teach or suggest anonymously capturing packets at the Internet Service Provider (ISP) point of presence (POP) that are identified as being associated with Web page requests anonymously. The Office Action cites Roth as column 8, lines 20-28 as disclosing IP data about a viewer, which may include CGI (common graphic interface) variables, Browser type (e.g. Netscape), viewers URL, high-level domain (.edu, .gov, .corn), OS of viewer (MAC, Windows, etc.), host, IP address, and URL of referring Web page. However, Roth does not disclose the capturing of packets associated with Web page request. Rather, Roth discloses that a Web page accessed by a viewer references an advertisement server and the advertisement server obtains information identifying the referring web page. However, the advertisement server does not capture packets associated with a request for the Web page.

Further, Roth does not disclose capturing packets at an Internet Service Provider (ISP) point of presence (POP). In Fig. 7, Roth shows a client browser 711 that sends web HTML references to a commercial Internet Service Provider (an ISP) 712. The ISP in turn sends an HTML reference to an advertising web server system. Bid input units send each proposed bid to bidding agents 730. Thus, the advertising web server system evaluate each proposed bid against the particular view-ops that are directed to each particular system. Thus, Roth fails to disclose capturing packets at an Internet Service Provider (ISP) point of presence (POP), but instead teaches forwarding packets on the advertising web server system.

Roth also fails to disclose, teach or suggest, for each user identifier correlated with the extracted IP address, storing the URL of the requested Web page and the user identifier

14

correlated with the extracted IP address at the ISP POP. Roth does not disclose extracting

an IP address at an ISP POP (see Fig. 7 discussion above). Roth also fails to disclose

correlating a user identifier with an extracted IP address. Instead, Roth merely discloses

the use of a "cookie" 11A, which provides information from browser 11 to the web server

system 16. The advertising web server system 16 uses information in cookie to identify the

user and web pages the user has accessed. However, Roth clearly fails to suggest storing

the URL of the requested Web page and the user identifier correlated with the extracted IP

address at the ISP POP.

Roth also fails to disclose, teach or suggest developing a user profile for the user

identifier, at the ISP POP, based on the extracted URLs associated with Web pages stored

at the ISP POP and requested by the user identifier. Roth discloses that user information is

maintained at a user information database maintained at the advertising web server system.

However, Roth does not disclose the development of a profile for the user identifier. Roth

does not disclose developing such a profile at the ISP POP.

Roth also fails to disclose, teach or suggest cross referencing Web site profiles with

the extracted URLs associated with Web pages requested by the user identifier to generate

an updated user profile, at the ISP POP, based on inferred user demographics of the Web

sites requested by the user identifier. Roth does not suggest updating user information at

an ISP POP or updating a profile cross referencing Web site profiles with the extracted

URLs associated with Web pages requested by the user identifier. Roth simply discloses

storing user information obtained through a cookie of the user.

Thus, Roth fails to disclose, teach or suggest the invention as defined in new independent claims 64, 80 and 109.

Armbruster fails to overcome the deficiencies of Roth. Armbruster is merely cited as disclosing monitoring packets at an Internet Service Provider (ISP) point of presence (POP), identifying monitored packets associated with Web page requests, extracting, at the ISP POP, a Uniform Resource Locator (URL) of the requested Web page and an IP address of the packets identified as being associated with the Web page request, processing the extracted IP address to correlate the extracted IP address with a user identifier using a cross-reference table at the ISP POP, associating each extracted URL with the user identifier correlated with the extracted IP address, developing a user profile for the user identifier, at the ISP POP, based on the extracted URLs associated with Web pages requested by the client having the user identifier and cross referencing Web site profiles with the extracted URLs associated with Web pages requested by the client having the user identifier to generate an updated user profile, at the ISP POP

The Final Office Action states that Armbruster discloses, at column 2, lines 66-67, that a content provider can control and monitor access to its site. However, claim 1 sets forth monitoring packets at an Internet Service Provider (ISP) point of presence (POP). The content provider is not an ISP POP. Thus, Armbruster fails to suggest monitoring packets at an Internet Service Provider (ISP) point of presence (POP).

Furthermore, Armbruster is completely silent regarding performing any of the above functions at an ISP POP. More specifically, Armbruster fails to disclose, teach or suggest anonymously capturing, at the ISP POP, packets identified as being associated with

Web page requests. Rather, Armbruster only discloses modifying URLs of cached data so that requests for such data are directed to the local cache or to the central caching server. However, Armbruster does not mention capturing packets associated with Web page requests anonymously.

The Advisory Action states that Armbruster discloses a cache located at an ISP's point-of-presence, wherein the ISP includes a local caching complex 10, consisting of servers and storage devices for identifying and storing cacheable web pages, filtering software, and web sites including the URLs associated with the cached items and forwarding packets to the ISP local cache. However, Armbruster merely discloses that caches at ISPs are updated from a central cache server. Thus, Armbruster fails to disclose, teach or suggest cross referencing Web site profiles with the extracted URLs associated with Web pages requested by the client having the user identifier to generate an updated user profile, at the ISP POP

Armbruster fails to disclose, teach or suggest processing the extracted IP address to correlate the extracted IP address with a user identifier using a cross-reference table at the ISP POP. Armbruster fails to mention correlating extracted IP addresses with a user identifier using a cross-reference table at the ISP POP.

Armbruster also fails to suggest determining a user identifier associated with the client correlated with the extracted IP address. Rather, Armbruster does not even mention user identifiers. Instead, Armbruster is merely concerned with being able to route a user to a central cache for data that is not maintained or available in a local cache.

Armbruster also fails to suggest developing a user profile for the user ID, at the ISP POP, based on the extracted URLs associated with Web pages requested by the user identifier. Again, Armbruster merely discloses routing a user to a central cache for data that is not maintained or available in a local cache.

Thus, Roth and Armbruster, alone or in combination, fail to disclose, teach or suggest the invention as defined in independent claims 64, 80 and 109.

Bull fails to overcome the deficiencies of Roth and Armbruster. Bull is merely cited as disclosing that the user's web viewing patterns are monitored and matched against software text agents to match a profile including user demographics. According to Bull, during a session or after a user discontinues use, the data viewed (recorded in the browsing activity datastore 240) is analyzed by the session profile update 2921 and the user profile datastore 210 is updated with keywords or personal search text agent datastore 232.

Accordingly, Bull merely creates a profile based on a user's viewing patterns. However, Bull fails to disclose extracting an IP address of the packets identified as being associated with the Web page request. Bull further fails to suggest processing the extracted IP address to correlate the extracted IP address with a client using a cross-reference table at the ISP POP. Rather, Bull develops a user profile based on data entered by the user and/or the viewing patterns of the user. Nevertheless, Bull fails to mention correlating an extracted IP address with a client using a cross-reference table at the ISP POP.

Bull also fails to disclose determining a user ID associated with the client correlated with the extracted IP address. Bull also fails to disclose storing the user ID associated with

the client correlated with the extracted IP address. Bull does not process the packets to identify a user ID using a cross-reference table for correlation with anonymous user IDs.

Bull further fails to suggest developing a user profile for the user ID based on the extracted URLs associated with Web pages requested by the client having the user IDs. Rather, Bull discloses that the user's viewing patterns may only be monitored if the user logs on to the system.

Bull further fails to disclose storing each URL associated with a Web site requested by a client and the user ID of that client. Again, Bull merely discloses that a user logs on to the system and, therefore, Bull fails to disclose determining the user ID of the client.

Thus, Roth, Armbruster and Bull, alone or in combination, fail to disclose, teach or suggest the invention as defined in new independent claims 64, 80 and 109.

Sheena fails to overcome the deficiencies of Roth, Armbruster and Bull. Sheena is merely cited as disclosing the use of an averaging algorithm to calculate a similarity factor between a pair of users. According to Sheena, the similarity between a pair of users may be calculated by averaging the squared difference between their ratings for mutually rated items. Thus, the similarity factor between user x and user y is calculated by subtracting, for each item rated by both users, the rating given to an item by user y from the rating given to that same item by user x and squaring the difference. The squared differences are summed and divided by the total number of items rated.

However, Sheena does not disclose the above-described functions occurring at an Internet Service Provider (ISP) point of presence (POP). Sheena also does not disclose capturing packets associated with Web page requests anonymously. Sheena does not

disclose determining a user ID associated with each IP address of a client requesting a Web page. Sheena still further fails to suggest cross referencing Web site profiles with the extracted URLs to generate an updated user profile based on inferred user demographics of the Web sites requested by the client having the user ID. Sheena simply does not disclose such cross-referencing.

Thus, Roth, Armbruster, Bull and Sheena, alone or in combination, fail to disclose, teach or suggest the invention as defined in new independent claims 64, 80 and 109.

Eldering fails to overcome the deficiencies of Roth, Armbruster, Bull and Sheena. Eldering is merely cited as disclosing the generation of a profile based on the purchase history of a consumer. To preserve privacy, Eldering discloses the records of Web sites a user has visited are erased after developing the user's profile. More specifically, Eldering discloses maintaining consumer privacy via private data networks.

However, Eldering does not disclose the above-described functions occurring at an Internet Service Provider (ISP) point of presence (POP). Eldering also does not disclose capturing packets associated with Web page requests anonymously.

Eldering does not disclose determining a user ID associated with each extracted IP address of a client requesting a Web page. Eldering further fails to disclose storing the user ID of that client. Eldering still further fails to suggest cross referencing Web site profiles with the extracted URLs to generate an updated user profile based on inferred user demographics of the Web sites requested by the client having the user ID. Eldering simply does not disclose such cross-referencing.

Thus, Roth, Armbruster, Bull, Sheena and Eldering, alone or in combination, fail to disclose, teach or suggest the invention as defined in new independent claims 64, 80 and 109.

Park fails to overcome the deficiencies of Roth, Armbruster, Bull, Sheena and Eldering. Park is merely cited as disclosing the transmitting of pop-up and banner advertisements to a display of a computer operated by the user.

However, Park does not disclose the above-described functions occurring at an Internet Service Provider (ISP) point of presence (POP). Park also does not disclose capturing packets associated with Web page requests anonymously. Park does not disclose determining a user ID associated with each extracted IP address of a client requesting a Web page.

Thus, Roth, Armbruster, Bull, Sheena, Eldering and Park, alone or in combination, fail to disclose, teach or suggest the invention as defined in new independent claims 64, 80 and 109.

Dependent claims 65-79 and 81-94 are also patentable over the references, because they incorporate all of the limitations of the corresponding independent claims 64 and 80, respectively. Further dependent claims 65-79 and 81-94 recite additional novel elements and limitations. Applicants reserve the right to argue independently the patentability of these additional novel aspects. Therefore, Applicants respectfully submit that dependent claims 65-79 and 81-94 are patentable over the cited references.
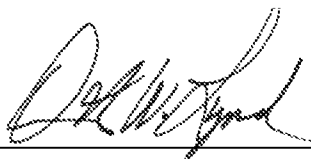
On the basis of the above amendments and remarks, it is respectfully submitted that the claims are in immediate condition for allowance. Accordingly, reconsideration of this application and its allowance are requested.

If a telephone conference would be helpful in resolving any issues concerning this communication, please contact Attorney for Applicant, David W. Lynch, at 865-380-5976. If necessary, the Commissioner is hereby authorized in this, concurrent, and future replies, to charge payment or credit any overpayment to Deposit Account No. 13-2725 for any additional fee required under 37 C.F.R. §§ 1.16 or 1.17; particularly, extension of time fees.

Respectfully submitted,

Merchant & Gould
P.O. Box 2903
Minneapolis, MN 55402-0903
(865) 380-5976

94140
PATENT TRADEMARK OFFICE

By: _____
Name: David W. Lynch
Reg. No.: 36,204